The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/09/2020

SUBJECT:
Multiple Vulnerabilities in Juniper Products Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Juniper products, the most severe of which could allow for remote code execution. Juniper is a vendor for IT, networking and cybersecurity solutions. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED
- Juniper Networks Junos OS
- Junos Space and Junos Space Director prior to 20.1R1
- Juniper Session and Resource Control prior to 4.12.0-R4, 4.13.0-R2
- Juniper Secure Analytics 7.3.0, 7.3.1, 7.3.2 versions prior to 7.3.2 Patch 7, 7.3.3 versions prior to 7.3.3 Patch 3

RISK:
Government:
- Large and medium government entities: **HIGH**
- Small government entities: **HIGH**

Businesses:
- Large and medium business entities: **HIGH**
- Small business entities: **HIGH**

Home Users: LOW

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Juniper products, the most severe of which could allow for remote code execution.

A full list of all vulnerabilities can be found at the link below:
https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Juniper to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Juniper:
https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11030&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11023&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11024&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11025&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11026&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11028&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11027&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11032&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11031&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11033&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11034&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11035&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11036&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11038&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11037&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11039&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11040&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11041&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11042&cat=SIRT_1&actp=LIST

http://www.us-cert.gov/tlp/